

(19)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

**EP 1 001 641 A2**

(12)

**EUROPEAN PATENT APPLICATION**

(43) Date of publication:  
17.05.2000 Bulletin 2000/20

(51) Int Cl.7: **H04Q 7/38**(21) Application number: **99308677.6**(22) Date of filing: **02.11.1999**

(84) Designated Contracting States:  
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE**  
Designated Extension States:  
**AL LT LV MK RO SI**

(72) Inventors:  
• Berenzweig, Adam L.  
New York, New York 10003 (US)  
• Brathwaite, Carlos Enrique  
Orangen, New Jersey 07050 (US)

(30) Priority: **09.11.1998 US 188816**

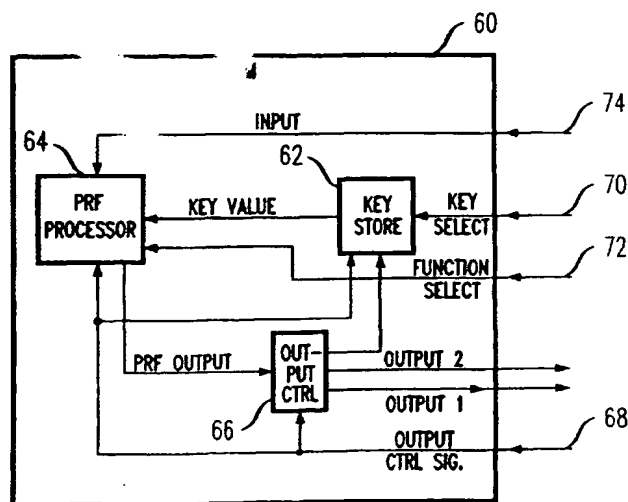
(74) Representative:  
**Buckley, Christopher Simon Thirsk et al**  
**Lucent Technologies (UK) Ltd,**  
**5 Mornington Road**  
**Woodford Green, Essex IG8 0TU (GB)**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**  
**Murray Hill, New Jersey 07974-0636 (US)**

**(54) Secure method for generating cryptographic function outputs**

(57) Data that indicates the use of a pseudorandom function output is used to modify at least one value used to produce the pseudorandom function output. In one embodiment, the output control signals provided to a User Identity Module (UIM) device are used as inputs to a pseudorandom function processor. As a result, the output provided by the processor differs based on whether the output from the processor is going to be stored in a key storage area or exported for use outside

the UIM. This technique solves the problem of the prior art by insuring that values that are exported or presented at the output of UIM module, are different than the values that are stored within the UIM module as key values. As a result, an attacker would receive values at the output of the UIM that are different than the values stored in the key storage unit and therefore, would not be able to impersonate the mobile terminal or compromise the privacy of the terminal's communications.

**FIG 4**

## Description

### Background of the Invention

### Field of the Invention

[0001] The present invention relates to communications; more specifically, the security of the authentication process used in communication systems.

### Description of the Related Art

[0002] FIG. 1 illustrates a base station 10, its associated cell 12 and mobile 14 within cell 12. When mobile 14 first registers or attempts communications with base station 10, base station 10 authenticates or verifies the mobile's identity before allowing the mobile access to the communication network. The authentication of mobile 14 involves communicating with authentication center 16. Authentication center 16 then accesses a home location register 22 which is associated with mobile 14. Home location register 22 may be associated with the terminal or mobile by an identifier such as the mobile's telephone number. The information contained in the home location register is used to generate encryption keys and other information. This information is used to supply base station 10 with information that is transmitted to mobile 14 so that mobile 14 can respond and thereby be authenticated as a mobile that is entitled to receive communication services.

[0003] FIGS. 2a and 2b illustrate the authentication process used for an IS41 compliant network. IS41 compliant networks are networks that use, for example, AMPS, TDMA or CDMA protocols. In this system, both the mobile and home location register contain a secret value called AKEY. Before the actual authentication process can start, a key update is performed by providing the mobile with keys that will be used with encryption functions for authentication and communication. The AKEY value stored in the home location register associated with the mobile is used to produce the keys. The keys values calculated are the SSDA (Shared Secret Data A) and SSDB (Shared Secret Data B) values. These values are calculated by performing the CAVE algorithm or function using a random number  $R_S$  as an input and the value AKEY as the key input. The CAVE algorithm is well known in the art and is specified in the IS41 standard. The network then updates the key values SSDA and SSDB that will be used by the mobile by transmitting  $R_S$  to the mobile. The mobile then calculates SSDA and SSDB in the same fashion as calculated by the authentication center. Now that the mobile and home location register both contain the SSDA and SSDB values, the authentication process may take place.

[0004] FIG. 2b illustrates how a mobile is authenticated to a network after both the mobile and home location register have received the keys SSDA and SSDB. The authentication center challenges the mobile by sending

a random number  $R_N$  to the mobile. At this point both the mobile and authentication center calculate the value AUTHR, where AUTHR is equal to the output of the CAVE algorithm using the random number  $R_N$  as an input and the SSDA value as the key input. The mobile then transmits the calculated value AUTHR to the authentication center. The authentication center compares its calculated value of AUTHR and the value received from the mobile. If the values match, the mobile is authenticated and it is given access to the network. In addition, both the mobile and the authentication center calculate the value of cipher key  $K_C$  where the value  $K_C$  is equal to the output of the CAVE algorithm using the value  $R_N$  as an input and the value SSDB as the key input. At this point, communications between the mobile and network are permitted and may be encrypted using a cryptographic function where the inputs are the message to be encrypted and the key value is  $K_C$ .

[0005] Since the values SSDA and SSDB are used to verify or authenticate the mobile terminal's identity, it is important that an imposter mobile terminal does not obtain these values. Additionally, the key value  $K_C$  is used for encrypting communications with the mobile terminal and if this value is obtained by an outsider, the privacy of the communications may be compromised.

[0006] FIG. 3 is a function block diagram of a user identity module or smart card that is typically used in communication devices. User identity module (UIM) 30 contains a key value storage memory 32 which is preferably a nonvolatile memory. Pseudorandom function (PRF) unit 34 contains a processor that executes pseudorandom functions such as cryptographic functions and one-way cryptographic functions or hash functions. Pseudorandom function unit 34 is used to generate an output on line 36 based on a key values provided by key storage unit 32, an input value received from an input to UIM 30 and a function select provided to UIM 30. The key value provided to PRF unit 34 is based on a key select input provided to UIM 30. PRF unit 34 selects a pseudorandom function to execute based on the function select input, and uses the input and key values as inputs to the selected pseudorandom function to produce an output on line 36. The output on line 36 is provided to either key storage area 32 where it is stored as a key value, or to the UIM output for export and use by the communication terminal containing UIM 30. The determination of whether to provide the outputs on line 36 to key store unit 32 or to the output of UIM 30 is made by output controller 40 based on an input received on line 42. This configuration is susceptible to an attack where an outsider provides UIM 30 with the inputs necessary to generate the values SSDA, SSDB or  $K_C$  while manipulating the values at input 42 so that the values SSDA, SSDB or  $K_C$  can be diverted to the output of the UIM rather than to key storage 32.

### Summary of the Invention

[0007] The present invention solves the aforementioned problem by using data that indicates the use of a pseudorandom function output to modify at least one value used to produce the pseudorandom function output. In one embodiment, the output control signals provided to a UIM device are used as inputs to a pseudorandom function processor. As a result, the output provided by the processor differs based on whether the output from the processor is going to be stored in a key storage area or exported for use outside the UIM. This technique solves the problem of the prior art by insuring that values that are exported or presented at the output of UIM module, are different than the values that are stored within the UIM module as key values. As a result, an attacker would receive values at the output of the UIM that are different than the values stored in the key storage unit and therefore, would not be able to impersonate the mobile terminal or compromise the privacy of the terminal's communications.

### Brief Description of the Drawings

[0008]

FIG. 1 illustrates the communication between a mobile and authentication center;  
FIGS. 2a and 2b illustrate the key update and authentication process for an IS41 compliant network;  
FIG. 3 illustrates a functional block diagram of a user identity module;  
FIG. 4 illustrates a functional block diagram of a user identity module where the output control changes the values produced by a pseudorandom function processor; and  
FIG. 5 illustrates how data indicative of the use of a pseudorandom function output is used to modify a value used to produce the pseudorandom function output.

### Detailed Description of the Invention

[0009] FIG. 4 illustrates a block diagram of a user identity module (UIM) 60 containing a key storage element 62, a pseudorandom function (PRF) processor 64 and an output controller 66. UIM module 60 may be fabricated on a single silicon device or in a sealed package. Key store device 62 may be implemented using a non-volatile memory such as an electrically erasable programmable read only memory (EEPROM). Pseudorandom function processor 64 may be implemented using a microprocessor or microcomputer that executes a program that implements one or more pseudorandom functions. The pseudorandom functions may be implemented in terms of an algorithm or a combination of an algorithm and a look-up table. Pseudorandom functions may be functions such as cryptographic functions and/or

one-way cryptographic functions such as hash functions. The pseudorandom functions may also be any of the well known pseudorandom functions specified in telecommunication standards such as IS41 or GSM. Processors that produce an output from a pseudorandom function are well known in the art and are used in many mobile communication terminals. Output controller 66 may be a switch or multiplexer that provides the output from PRF processor to key storage unit 62 for storage or to the output of UIM 60 for export based on signals provided on input 68. The control signals received on input 68 are also provided as an input to pseudorandom function processor 64 where the signals may be used to modify values that are used to produce a pseudorandom function output. Key storage unit 62 provides a key value to PRF processor 64 based on inputs received on input 70. The output control signals may also be provided as an input to key storage unit 62 and used to modify the identifier or pointer used to select the key value supplied to PRF processor 64.

[0010] FIG. 5 illustrates the process by which PRF processor 64 produces an output. The pseudorandom random function identifier data or value from function select input 72 is illustrated by bit field 100, the input data or value from input 74 is illustrated as bit field 102, the key pointer data or value from input 70 is illustrated as bit field 104 and the output control data or value from input 68 is illustrated as bit field 106. Output control field 106 may be used to modify the output produced by PRF processor 64 in several ways. For example, one or more bits of output control field 106 may be used to modify the bits in key select field 104 which is used as a pointer to key values in key storage 62. It is also possible for one or more bits of output control field 106 to modify input field 102 or modify function select field 100. The modification may include an arithmetic or logic operation, or a simple concatenation of bits.

[0011] PRF processor 64 selects a pseudorandom function F in step 110. This selection is based on bit field 100 which may be modified as discussed earlier using one or more bits from output control field 106. In step 112, PRF processor 64 inputs a key value from key storage unit 62. The pointer which identified the key value for step 112 may be modified using one or more bits of output control field 106. It is also possible for processor 64 to execute step 114 and to modify the key value received from key storage 62 using one or more bits from output control field 106. As discussed above, the modification may involve an arithmetic or logic operation, or a simple concatenation of bits. In step 116, PRF processor 64 inputs the values from input field 102. This field may also be modified using one or more bits from output control field 106. In step 118, PRF processor 64 executes the pseudorandom function using the key value K and the input value I to produce an output which is then sent to output control unit 66 in step 120.

**Claims**

1. A method for producing an output using a pseudorandom function, comprising the steps of:

receiving a value used as an input to produce a pseudorandom function output;  
modifying the value based on a use of the pseudorandom function output to produce a modified value; and  
producing a pseudorandom function output using the modified value.

2. The method of claim 1, wherein the value identifies a key value to be used as an input to the pseudorandom function.

3. The method of claim 1, wherein the value is a key value to be used as an input to the pseudorandom function.

4. The method of claim 1, wherein the value identifies one of a plurality of pseudorandom functions.

5. The method of claim 1, further comprising the step of receiving data indicating that the output of the pseudorandom function is to be stored.

6. The method of claim 1, further comprising the step of receiving data indicating that the output of the pseudorandom function is to be stored as a key value.

7. The method of claim 1, further comprising the step of receiving data indicating that the output of the pseudorandom function is to be exported.

8. A method for producing an output using a pseudorandom function, comprising the steps of:

receiving data, where the data indicates a use of a pseudorandom function output, and where the data comprises at least one of an input value, a key value, a key pointer value and a pseudorandom function identifier value;  
modifying at least one of the input value, the key value, the key pointer value and the pseudorandom function identifier value, based on the use of the pseudorandom function output to produce at least one modified value; and  
producing a pseudorandom function output using at least one modified value.

9. The method of claim 8, wherein the data indicates that the output of the pseudorandom function is to be stored.

10. The method of claim 8, wherein the data indicates

that the output of the pseudorandom function is to be stored as a key.

11. The method of claim 8, wherein the data indicates that the output of the pseudorandom function is to be exported.

FIG 1

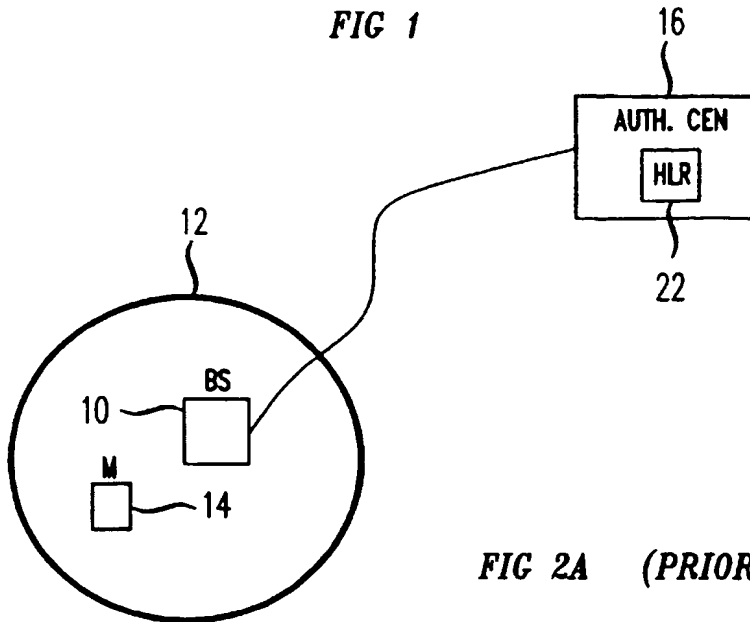


FIG 2A (PRIOR ART)

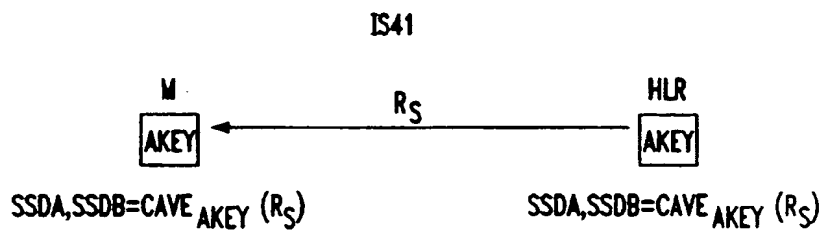
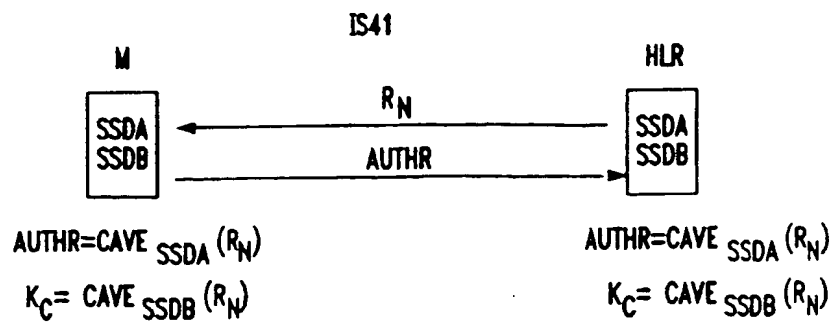
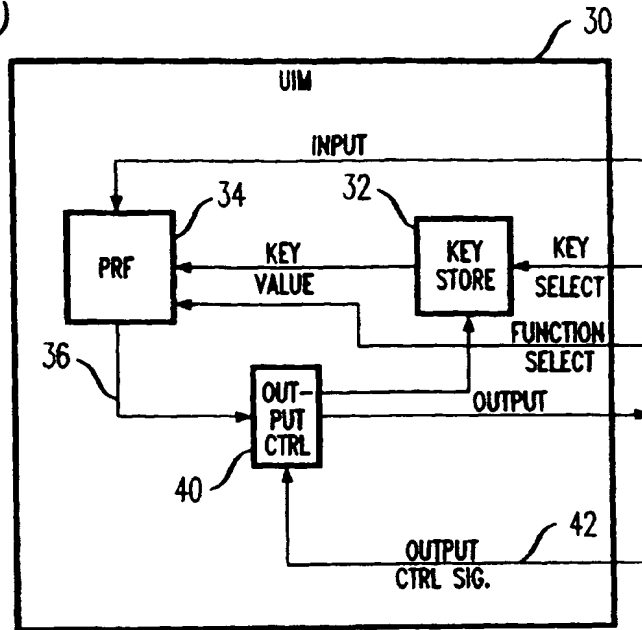


FIG 2B (PRIOR ART)



**FIG 3**  
(PRIOR ART)



**FIG 4**

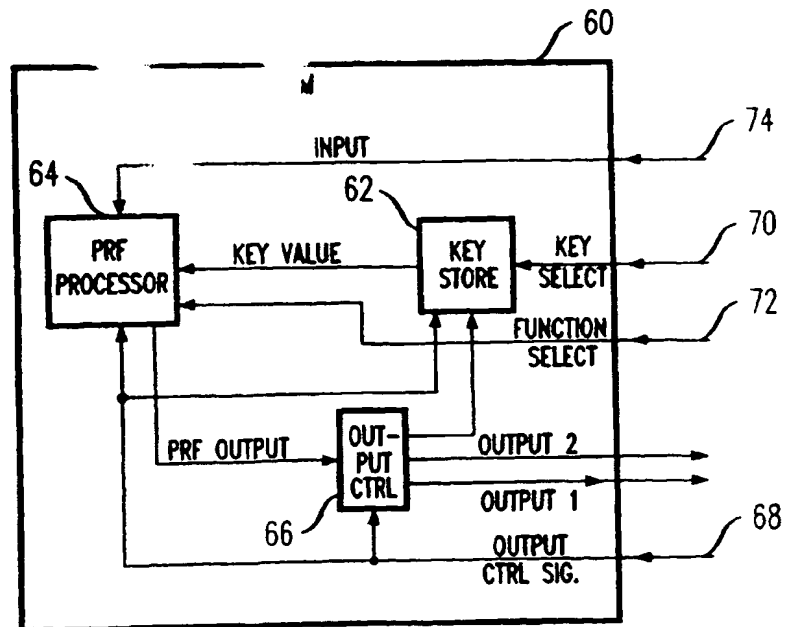
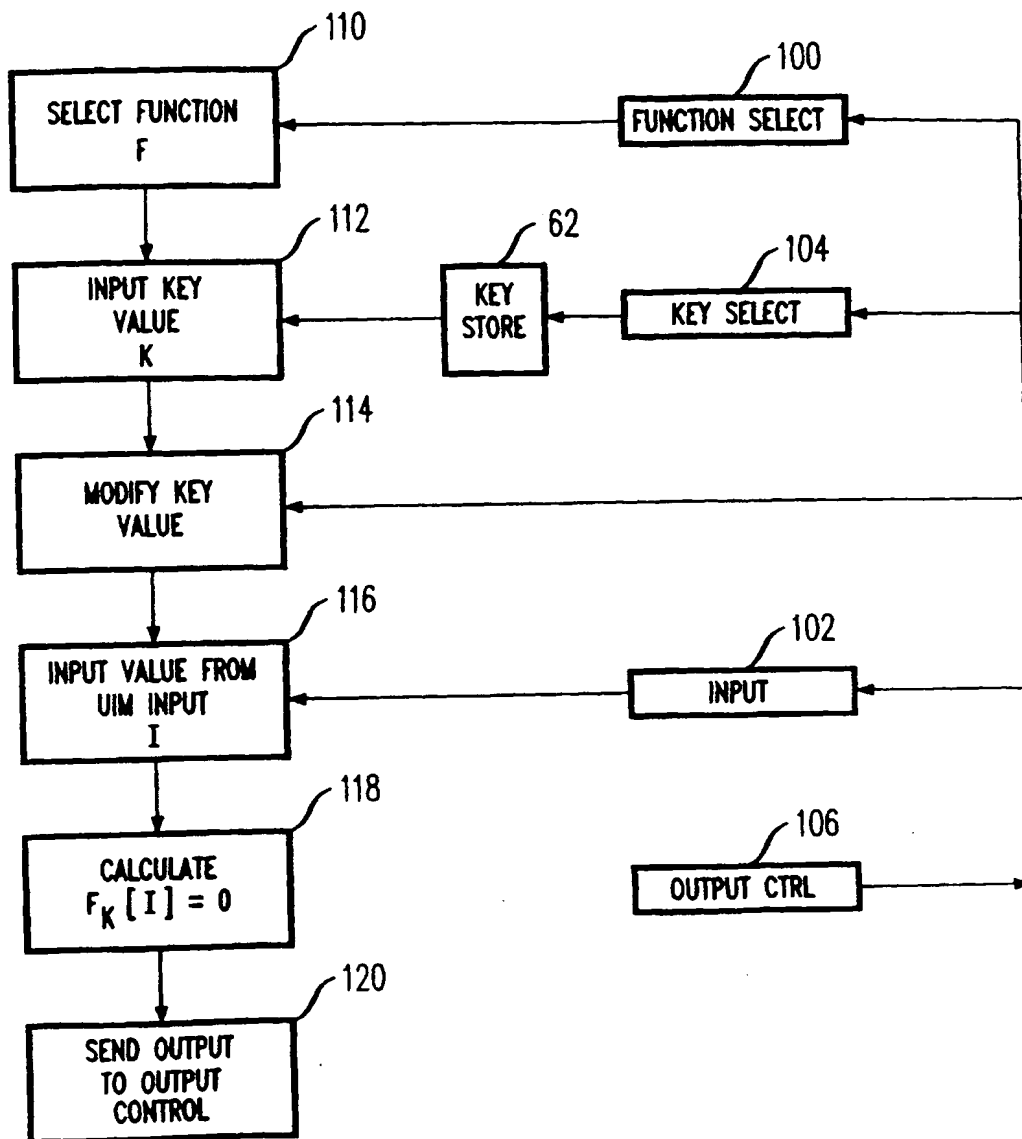


FIG 5



(19)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

EP 1 001 641 A3

(12)

## EUROPEAN PATENT APPLICATION

(88) Date of publication A3:  
03.01.2001 Bulletin 2001/01

(51) Int Cl.7: H04Q 7/38

(43) Date of publication A2:  
17.05.2000 Bulletin 2000/20

(21) Application number: 99308677.6

(22) Date of filing: 02.11.1999

(84) Designated Contracting States:  
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE  
Designated Extension States:  
AL LT LV MK RO SI

(72) Inventors:  
• Berenzweig, Adam L.  
New York, New York 10003 (US)  
• Brathwalte, Carlos Enrique  
Orangeney, New Jersey 07050 (US)

(30) Priority: 09.11.1998 US 188816

(74) Representative:  
Buckley, Christopher Simon Thirsk et al  
Lucent Technologies (UK) Ltd,  
5 Mornington Road  
Woodford Green, Essex IG8 0TU (GB)

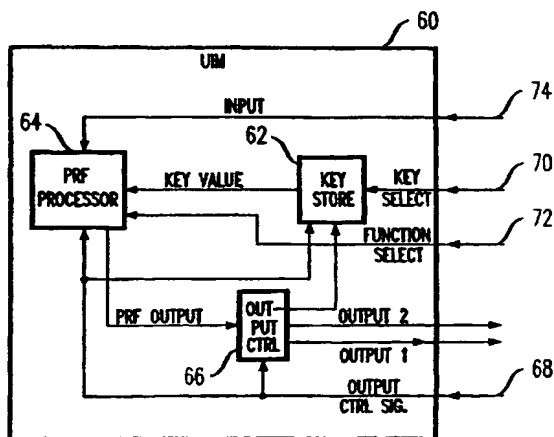
(71) Applicant: LUCENT TECHNOLOGIES INC.  
Murray Hill, New Jersey 07974-0636 (US)

### (54) Secure method for generating cryptographic function outputs

(57) Data that indicates the use of a pseudorandom function output is used to modify at least one value used to produce the pseudorandom function output. In one embodiment, the output control signals provided to a User Identity Module (UIM) device are used as inputs to a pseudorandom function processor. As a result, the output provided by the processor differs based on whether the output from the processor is going to be stored in a key storage area or exported for use outside

the UIM. This technique solves the problem of the prior art by insuring that values that are exported or presented at the output of UIM module, are different than the values that are stored within the UIM module as key values. As a result, an attacker would receive values at the output of the UIM that are different than the values stored in the key storage unit and therefore, would not be able to impersonate the mobile terminal or compromise the privacy of the terminal's communications.

FIG 4







European Patent  
Office

## EUROPEAN SEARCH REPORT

Application Number  
EP 99 30 8677

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 421 409 A (IBM) 10 April 1991 (1991-04-10) * claim 15 *	1,8	H04Q7/38
A	PATEL S: "WEAKNESS OF NORTH AMERICAN WIRELESS AUTHENTICATION PROTOCOL" IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, vol. 4, no. 3, 1 June 1997 (1997-06-01), pages 40-44, XP000655315 ISSN: 1070-9916 * page 40 - page 44 *	1,8	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			H04Q 607F
The present search report has been drawn up for all claims			
Place of search <b>THE HAGUE</b>		Date of completion of the search <b>9 November 2000</b>	Examiner <b>M. García</b>
<p><b>CATEGORY OF CITED DOCUMENTS</b></p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons A : member of the same patent family, corresponding document</p>			

EPO FORM 1503 (03.02 (Rev.03))

EP 1 001 641 A3

**ANNEX TO THE EUROPEAN SEARCH REPORT  
ON EUROPEAN PATENT APPLICATION NO.**

EP 99 30 8677

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.  
The members are as contained in the European Patent Office EDP file on  
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-11-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0421409 A	10-04-1991	US 5048085 A	10-09-1991
		CA 2026739 A,C	07-04-1991
		JP 3237551 A	23-10-1991
		US 5148481 A	15-09-1992

EPD FORM P0488

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82